09-23-05

PATENT AF

JFW

EXPRESS MAIL CERTIFICATE OF MAILING

Express Mail Certificate No. EV520756985US

I hereby certify that the *attached* correspondence comprising:

1. TRANSMITTAL OF BRIEF ON APPEAL (37 C.F.R. § 1.192) (2 pages) (in duplicate); Return Postcard

is being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" addressed to:

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on September 21, 2005

Kathy Raymond

Kathy Raymond

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant :	Marcey L. Kelly, et al.	Docket No. :	IL-10707
Serial No. :	09/964,029	Art Unit :	2161
Filed :	09/26/2001	Examiner :	Etienne Pierre Leroux
For :	SOFTWARE DISTRIBUTION SYSTEM		

TRANSMITTAL OF BRIEF ON APPEAL (PATENT APPLICATION - 37 CFR 192)

Transmitted herewith in **duplicate** is the **BRIEF ON APPEAL** in this application with respect to the Notice of Appeal filed on August 2, 2005.

The item(s) checked below are appropriate:

1. **STATUS OF APPLICANT**
   This application is on behalf of
   - ☐ other than a small entity.
   - ■ a small entity.
     A verified statement
     - ☐ is attached
     - ■ already filed.

2. **FEE FOR FILING APPEAL BRIEF**
   Pursuant to 37 CFR 1.17(e) the fee for filing the Appeal Brief is:
   - ■ small entity $250.00
   - ☐ other than a small entity $500.00

   Appeal Brief fee due **$250.00**

3. **EXTENSION OF TIME**

❑ Applicant petitions for an extension of time under 37 CFR 1.136

Calculation of extension fee (37 CFR 1.17(a)-(d)):

	Total months requested	Fee for other than small entity	Fee for small entity
☐	one month	$120.00	$60.00
☐	two month	$450.00	$225.00
☐	three month	$1,020.00	$510.00
☐	four month	$1,590.00	$795.00
☐	five month	$2,160.00	$1,080.00
		Fee	**$000.00**

4. **FEE PAYMENT**

■ Charge Account No. 12-0695 in the amount of **$250.00**.

■ **Charge Account No. 12-0695 for any additional extension and/or fee required or credit for any excess fee paid.**

Eddie E. Scott
Agent for Applicant(s)
Reg. No. 25,220
Tel. No. (925) 424-6897

Date: September 22, 2005

EXPRESS MAIL CERTIFICATE OF MAILING

Express Mail Certificate No. EV708707598US

I hereby certify that the *attached* correspondence comprising:
1. Appellant's Brief (16 pages), 2. Return Postcard
is being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" addressed to:

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on September 21, 2005

Kathy Raymond

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant :	Marcey L. Kelly, et al.	Docket No. :	IL-10707
Serial No. :	09/964,029	Art Unit :	2161
Filed :	09/26/2001	Examiner :	Etienne Pierre Leroux
For :	SOFTWARE DISTRIBUTION SYSTEM		

Honorable Commissioner for Patents
Alexandria, VA 22313-1450

Attention: Board of Patent Appeals and Interferences

Dear Sir:

APPELLANT'S BRIEF (37 C.F.R. § 1.192)

This brief is submitted in support of appellant's notice of appeal from the decision of the Examiner, mailed May 5, 2005 finally rejecting claim 6 of the subject application. Appellant's notice of appeal was mailed August 2, 2005.

One copy of the brief is being transmitted per 37 C.F.R. § 41.37.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is:

The Regents of the University of California and the United States of America as represented by the United States Department of Energy (DOE) by virtue of an assignment by the inventor as duly recorded in the Assignment Branch of the U.S. Patent and Trademark Office.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF CLAIMS

The application as originally filed contained claims 1-17.

Claims 1-5 and 7-17 have been cancelled.

The claim on appeal is claim 6.

Claim 6 on appeal is reproduced in the Appendix.

IV. STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the final rejection mailed May 5, 2005.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The invention defined by Appellant's claim 6 on appeal is described in Appellants' original specification and drawings. Appellants' specification and drawings, i.e., the original application, was published as United States Patent Application No. 2002/0174422. The text of Appellants' original application is

cited with paragraphs in brackets [....] according to Application No. 2002/0174422.

[0034] System software is constantly changing, making it difficult to maintain the integrity of the software. ....

[0044] The present invention provides a system for secure software distribution including determining which patches have been applied to a system. Determining which patches should be or should have been applied to a system. Collecting patches from the supported vendors by downloading them from the vendor's ftp sites. Interpreting the operating system type, version and architecture the patch applies to; how much memory and disk space is needed to install the patch; dependencies on other layered products, patches, or upgrades; and which files and directories are affected by the installation of a patch. Installing and possibly backing-out the patches.

[0026] Certain embodiments of the system are known as SafePatch secure distribution software system. This system provides automated analysis, distribution, and notification and installation of security patches on network-based computer systems. SafePatch determines what patches need to be installed. For the patches that are installed, SafePatch checks the permissions and ownership of the files referenced in the patch and ensures that the system software is authentic. SafePatch detects patch deficiencies and distributes needed patches as well as the appropriate installation script to client's systems, and optionally installs those patches.

The elements of Appellant's claim 6 on appeal are "read on" Appellant's original specification in the comparison below. The left column contains the elements of Appellants' claim 6 and the right column shows the text of Appellants' original application.

Claim 6	Appellants' Application 2002/0174422
Claim 6. A computer-implemented method of secure distribution of vendor's upgrades and vendor's software patch or vendor's software patches to client's systems; wherein the method utilizes such thing as vendors, vendor's ftp sites, system software, files, permissions referenced in the files, ownership of files referenced in the vendors' software patch, needed vendor's software patches, not needed vendor's software patches, directories, operating system type, operating system version, operating system architecture, memory, disk space, other layered products, other patches, and other software upgrades; comprising the steps of: determining which of the vendor's software patches should be applied to the client's systems, collecting the vendor's software patches from the vendors by downloading them from the vendor's ftp sites, interpreting which of the files will be affected by installation of the vendor's software patches, interpreting which of the directories will be affected by the installation of the vendor's software patches, interpreting the operating system type, version and architecture the vendor's software patches apply to, interpreting dependencies on the other layered products, determining which of the vendor's upgrades and the vendor's software patches have been applied to the client's systems,	[Pages 14 & 15] Original claims 1-17 [0046] Referring now to the drawings, and in particular to FIG. 1, ... Collecting patches from most vendors by downloading them from the vendor's ftp sites, interpreting the operating system type, version and architecture the patch applies to, how much memory and disk space is needed to install the patch, dependencies on other layered products, patches and which files and directories are affected by the installation of a patch. Installing and possibly backing- out patches. [0051] In addition to collecting patches, the SafePatch Server is responsible for evaluating target systems and installing patches on these systems. .... The owner, group, permissions, and checksum (for files only) for each file or directory on the list is checked against the owner, group, permissions, and checksums of the respective directory or file on the target system. .... [0169] The present invention provides a computer-implemented method of secure distribution and installation of vendor software patches onto client systems. The method includes determining which vendor's patches have been applied to a system and installing vendor's patches on a system. The method includes determining which patches should be or should have been applied to a system. The method includes backing out undesirable patches from a system. The method includes collecting patches from most vendors by downloading them from the vendor's ftp sites. The method includes interpreting the operating system type. The method includes interpreting the operating system version. The method includes interpreting the operating system architecture the patch applies to. The method includes determining how much memory is needed to install said patch. The method includes determining how dependencies on other layered products affect the installation of a patch. The method includes determining how dependencies on other upgrades or patches affect the installation of a patch, determining which files are affected by the installation of a patch, and determining which directories are affected by the installation of a patch.

Claim 6 (Continued)

determining which of the vendor's upgrades and the vendor's software patches should be or should have been applied to the clients systems,

collection of the vendor's software patches and the vendor's upgrades from the vendors and downloading the vendor's software patches and the vendor's upgrades to the client systems, interpreting the operating system type,

interpreting the operating system version,

interpreting the operating system architecture the vendor's software patch applies to,

determining how much of the memory is needed to install the vendor's software patch and the vendor's upgrades,

interpreting how much of the memory and of the disk space is needed to install the vendor's upgrades and installing the vendor's software patches,

determining how dependencies on the other layered products affect the installation of the vendor's software patches and the vendor's upgrades,

determining how dependencies on the other patches, or the other software upgrades affect the installation of the software patch,

determining how dependencies on the other software upgrades affect the installation of the vendor's software patch,

determining which of the files will be affected by the installation of the vendor's software patch,

determining which of the directories will be affected by the installation of the vendor's software patch,

Appellants' Application 2002/0174422

[Pages 14 & 15] Original claims 1-17

[0046] Referring now to the drawings, and in particular to FIG. 1, ... Collecting patches from most vendors by downloading them from the vendor's ftp sites, interpreting the operating system type, version and architecture the patch applies to, how much memory and disk space is needed to install the patch, dependencies on other layered products, patches and which files and directories are affected by the installation of a patch. Installing and possibly backing- out patches.

[0051] In addition to collecting patches, the SafePatch Server is responsible for evaluating target systems and installing patches on these systems. .... The owner, group, permissions, and checksum (for files only) for each file or directory on the list is checked against the owner, group, permissions, and checksums of the respective directory or file on the target system. ....

[0169] The present invention provides a computer-implemented method of secure distribution and installation of vendor software patches onto client systems. The method includes determining which vendor's patches have been applied to a system and installing vendor's patches on a system. The method includes determining which patches should be or should have been applied to a system. The method includes backing out undesirable patches from a system. The method includes collecting patches from most vendors by downloading them from the vendor's ftp sites. The method includes interpreting the operating system type. The method includes interpreting the operating system version. The method includes interpreting the operating system architecture the patch applies to. The method includes determining how much memory is needed to install said patch. The method includes determining how dependencies on other layered products affect the installation of a patch. The method includes determining how dependencies on other upgrades or patches affect the installation of a patch, determining which files are affected by the installation of a patch, and determining which directories are affected by the installation of a patch.

Claim 6 (Continued)	Appellants' Application 2002/0174422
backing-out the vendor's software patches that have been applied to the client's systems, checking the permissions and the ownership of the files referenced in the vendors' software patch and ensuring that the system software is authentic, determining which of the vendor's software patches should be installed by determining the needed vendor's software patches and the not needed vendor's software patches, distributing the needed the vendor's software patches to the client's systems, and installing the needed vendor's software patches.	[Pages 14 & 15] Original claims 1-17 [0046] Referring now to the drawings, and in particular to FIG. 1, ... Collecting patches from most vendors by downloading them from the vendor's ftp sites, interpreting the operating system type, version and architecture the patch applies to, how much memory and disk space is needed to install the patch, dependencies on other layered products, patches and which files and directories are affected by the installation of a patch. Installing and possibly backing- out patches. [0051] In addition to collecting patches, the SafePatch Server is responsible for evaluating target systems and installing patches on these systems. .... The owner, group, permissions, and checksum (for files only) for each file or directory on the list is checked against the owner, group, permissions, and checksums of the respective directory or file on the target system. .... [0169] The present invention provides a computer-implemented method of secure distribution and installation of vendor software patches onto client systems. The method includes determining which vendor's patches have been applied to a system and installing vendor's patches on a system. The method includes determining which patches should be or should have been applied to a system. The method includes backing out undesirable patches from a system. The method includes collecting patches from most vendors by downloading them from the vendor's ftp sites. The method includes interpreting the operating system type. The method includes interpreting the operating system version. The method includes interpreting the operating system architecture the patch applies to. The method includes determining how much memory is needed to install said patch. The method includes determining how dependencies on other layered products affect the installation of a patch. The method includes determining how dependencies on other upgrades or patches affect the installation of a patch, determining which files are affected by the installation of a patch, and determining which directories are affected by the installation of a patch.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Final Rejection Office Action mailed May 5, 2005 rejected claim 6 under 35 U.S.C. 102(b) as allegedly being anticipated by the Bartoletti et al reference (Conference Publication: Secure Software System by T. Bartoletti et al). The issue presented for review is whether claim 6 is anticipated by the Bartoletti et al reference.

VII. ARGUMENT

Appellants will show that specific elements of claim 6 are not found in the Bartoletti et al reference. Appellants will also show that the combination of elements of claim 6 is not found in the Bartoletti et al reference. In addition, Appellants will also show that the Bartoletti et al reference is a non-enabling reference and does not anticipate claim 6.

The Bartoletti Reference is a preliminary report by Appellants Marcey L. Kelley, Lauri A. Dobbs, and Tony Bartoletti describing problems that were expected to be encountered in a project that was just starting and the approach the inventors intended to use in solving the problems. The Bartoletti Reference is much shorter than Appellants' patent application and clearly does not include specific elements of claim 6 or the combination of elements of claim 6.

Proving that specific elements are not shown in a reference is the difficult exercise of proving a negative. Appellants argue that it is the Examiner's burden to show that all the elements of a claim are included in a reference. None-the-less, Appellants will provide a showing that elements of Appellants' claim 6 are missing from the Bartoletti et al reference and that the Bartoletti et al reference does not show the combination of elements of claim 6.

Individual elements of Appellants' claim 6 that are missing from the Bartoletti et al reference will be designated "Missing Element." Appellants will identify "Missing Elements" and demonstrate that they are missing from the Bartoletti et al reference. The standard for a 35 USC §102 rejection is stated in RCA Corp. v. Applied Digital Systems, Inc., 221PQ 385, 388 (d. Cir. 1984) "Anticipation is established only when a single prior art reference discloses, either expressly or under principles of inherency, each and every element of a claimed invention." For Appellants to succeed in this Appeal it is only necessary for Appellants to successfully identify a single "Missing Element."

Appellants' claim 6 is "a computer-implemented method of secure distribution of vendor's upgrades and vendor's software patch or vendor's software patches to client's systems." The method of claim 6 includes twenty three individual elements or steps.

MISSING ELEMENT #20 - On page 3, lines 19 & 20, of the Final Rejection Office Action mailed May 5, 2005, it was alleged that the Bartoletti et al reference discloses Appellants following claim element #20,

> "checking the permissions and the ownership of the files referenced in the vendors' software patch and ensuring that the system software is authentic." (Missing Element #20)

The Bartoletti et al reference does not disclose Missing Element #20. The portion of the Bartoletti et al reference relied upon in the Final Rejection Office Action mailed May 5, 2005 is quoted below.

> "A patch specification contains information such as the operating system type, version, and architecture as well as the permissions and ownership for each file and directory manipulated by the patch." (Page 5, paragraph 1, lines 10-13, Secure Software Distribution System by Tony Bartoletti, Lauri A. Dobbs, and Marcey Kelley, National Information Systems Security Conference Baltimore, MD, October 6-7, 1997)

Appellants claim element #20 requires two positive separate actions, "checking the permissions and the ownership of the files referenced in the vendors' software patch," and "ensuring that the system software is authentic." The portion of the Bartoletti et al reference as quoted above does not disclose these two positive separate actions. In particular, the Bartoletti et al reference does not disclose the portion of claim element #20 (Missing Element #20), "ensuring that the system software is authentic."

MISSING ELEMENT #21 - On page 3, lines 21 & 22, of the Final Rejection Office Action mailed May 5, 2005, it was alleged that the Bartoletti et al reference discloses Appellants following claim element #21,

> "determining which of the vendor's software patches should be installed by determining the needed vendor's software patches and the not needed vendor's software patches." (Missing Element #21)

The Bartoletti et al reference does not disclose Missing Element #21. The portion of the Bartoletti et al reference relied upon in the Final Rejection Office Action mailed May 5, 2005 is quoted below.

> "From this information, the SSDS Server can determine which patches need to be installed on the target system in order to bring it up-to-date." (Page 6, paragraph 2, lines 15-17, Secure Software Distribution System by Tony Bartoletti, Lauri A. Dobbs, and Marcey Kelley, National Information Systems Security Conference Baltimore, MD, October 6-7, 1997)

Appellants claim element #21 requires two positive separate actions, "determining which of the vendor's software patches should be installed by determining the needed vendor's software patches," .... "and the not needed vendor's software patches." The portion of the Bartoletti et al reference as quoted above does not disclose these two positive separate actions. In particular, the Bartoletti et al reference does not disclose the portion of claim element #21, "and the not needed vendor's software patches."

MISSING ELEMENT #22 - On page 4, lines 1 & 2, of the Final Rejection Office Action mailed May 5, 2005, it was alleged that the Bartoletti et al reference discloses Appellants following claim element #22,

> "distributing the needed vendor's software patches to the client's systems." (Missing Element #22)

The Bartoletti et al reference does not disclose Missing Element #22. The portion of the Bartoletti et al reference relied upon in the Final Rejection Office Action mailed May 5, 2005 is quoted below.

> "The system administrator can choose to have SSDS install patches immediately after the evaluation or at some later date and time. The system administrator can also choose not to have SSDS install the patches and instead report on the patches needed. This allows for the system administrators to dictate which actions SSDS is to perform on a system." (Page 6, paragraph 2, lines 18-20, Secure Software Distribution System by Tony Bartoletti, Lauri A. Dobbs, and Marcey Kelley, National Information Systems Security Conference Baltimore, MD, October 6-7, 1997)

Appellants claim element #22 requires, "distributing the needed vendor's software patches to the client's systems." The portion of the Bartoletti et al reference as quoted above does not disclose Missing Element #22.

COMBINATION OF ELEMENTS ARE NOT IN BARTOLETTI ET AL

Appellants' combination of elements in claim 6 are not found in the Bartoletti et al reference. Appellants' claim 6 is "a computer-implemented method of secure distribution of vendor's upgrades and vendor's software patch or vendor's software patches to client's systems" that includes a combination of twenty three individual elements or steps. The Bartoletti Reference describes problems that were expected to be encountered in a project that was just starting and the approach the inventors intended to use in solving the problems. The Bartoletti Reference does not describe a computer-implemented method of secure distribution of vendor's upgrades and vendor's software patch or

vendor's software patches to client's systems that includes Appellants' specific combination of twenty three individual steps.

NON-ENABLING REFERENCE - The Bartoletti reference is not an "enabled reference." The invention defined by the method steps of the claims on appeal is not supported in the Bartoletti Reference by a description of how the method is implemented. As stated in the Bartoletti Reference on page 6, lines 3-4, "The goal of the project is to develop a proof-of –concept prototype over several phases of development." McCarthy's Desk Encyclopedia of Intellectual Property, on page 113, in the description of enabling prior art, "To qualify as prior art, a reference must be enabling...." Prior art under 35 USC 102(b) must sufficiently describe the claimed invention to have placed the public in possession of it..." In re Donohue, 766 F. 2nd 531, 266 USPQ 619, 612 (Fed. Cir. 1985)

It is respectfully requested that claim 6 on appeal be allowed.

Respectfully submitted,

By: _____

Eddie E. Scott
University of California (LLNL)
7000 East Avenue, Mail Code L-703
Livermore, CA 94550
Attorney for Appellants
Registration No. 25,220
Telephone No. (925) 424-6897

Date: September 27, 2001

VIII. CLAIMS APPENDIX

Claim 6. (Previously Presented) A computer-implemented method of secure distribution of vendor's upgrades and vendor's software patch or vendor's software patches to client's systems; wherein the method utilizes such thing as vendors, vendor's ftp sites, system software, files, permissions referenced in the files, ownership of files referenced in the vendors' software patch, needed vendor's software patches, not needed vendor's software patches, directories, operating system type, operating system version, operating system architecture, memory, disk space, other layered products, other patches, and other software upgrades; comprising the steps of:

determining which of the vendor's software patches should be applied to the client's systems,

collecting the vendor's software patches from the vendors by downloading them from the vendor's ftp sites,

interpreting which of the files will be affected by installation of the vendor's software patches,

interpreting which of the directories will be affected by the installation of the vendor's software patches,

interpreting the operating system type, version and architecture the vendor's software patches apply to,

interpreting dependencies on the other layered products,

determining which of the vendor's upgrades and the vendor's software patches have been applied to the client's systems,

determining which of the vendor's upgrades and the vendor's software patches should be or should have been applied to the clients systems,

collection of the vendor's software patches and the vendor's upgrades from the vendors and downloading the vendor's software patches and the vendor's upgrades to the client systems,

interpreting the operating system type,

interpreting the operating system version,

interpreting the operating system architecture the vendor's software patch applies to,

determining how much of the memory is needed to install the vendor's software patch and the vendor's upgrades,

interpreting how much of the memory and of the disk space is needed to install the vendor's upgrades and installing the vendor's software patches,

determining how dependencies on the other layered products affect the installation of the vendor's software patches and the vendor's upgrades,

determining how dependencies on the other patches, or the other software upgrades affect the installation of the software patch,

determining how dependencies on the other software upgrades affect the installation of the vendor's software patch,

determining which of the files will be affected by the installation of the vendor's software patch,

determining which of the directories will be affected by the installation of the vendor's software patch,

backing-out the vendor's software patches that have been applied to the client's systems,

checking the permissions and the ownership of the files referenced in the vendors' software patch and ensuring that the system software is authentic,

determining which of the vendor's software patches should be installed by determining the needed vendor's software patches and the not needed vendor's software patches,

distributing the needed vendor's software patches to the client's systems, and

installing the needed vendor's software patches.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDING APPENDIX

None.